10057465

Refine Search

Terms	Documents
6529726.pn.	2

Database:

US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search:

L13

Refine Search

Recall Text ⬍   Clear   Interrupt

Search History

DATE: Thursday, April 14, 2005   Printable Copy   Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L13	6529726.pn.	2	L13
L12	L10 and (cell$ with authori$)	1	L12
L11	L10 and (cell$ with number)	6	L11
L10	L3 and transaction and (approv$ or authori$)	610	L10
L9	L3 and 6529726.pn.	0	L9
L8	L4 and 6529726.pn.	0	L8
L7	L4 and 705/44.ccls.	23	L7
L6	L4 and 705/44.ccls.5	12933711	L6
L5	L4 and (cell$ with number)	1	L5
L4	L3 and transaction and (charg$ near2 card) and (approv$ or authori$)	87	L4
L3	L2 and @ad<=19990302	1060	L3
L2	705/35,39-41,44.ccls.	3869	L2

Hit List

Search Results - Record(s) 1 through 2 of 2 returned.

☐ 1. Document ID: US 6529726 B1

Using default format because multiple data bases are involved.

L13: Entry 1 of 2   File: USPT   Mar 4, 2003

```
US-PAT-NO: 6529726
DOCUMENT-IDENTIFIER: US 6529726 B1

TITLE: Method of notifying a wireless subscriber as to call payment
responsibilities

DATE-ISSUED: March 4, 2003

INVENTOR-INFORMATION:
NAME                    CITY          STATE     ZIP CODE     COUNTRY
Rhodes; Jeffrey         Redmond       WA

US-CL-CURRENT: 455/406; 455/414.1, 455/415, 455/560, 455/566, 455/567
```

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De |

☐ 2. Document ID: US 6529726 B1

L13: Entry 2 of 2   File: DWPI   Mar 4, 2003

```
DERWENT-ACC-NO: 2003-379380
DERWENT-WEEK: 200518
COPYRIGHT 2005 DERWENT INFORMATION LTD

TITLE: Call payment responsibility notification method in mobile communication,
involves routing called party identification notification message to mobile
telephone, charging calling party for call, and connecting call to mobile telephone
```

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De |

Terms	Documents
6529726.pn.	2

L11: Entry 2 of 6   File: USPT   Nov 23, 1999

US-PAT-NO: 5991749
DOCUMENT-IDENTIFIER: US 5991749 A
** See image for **Certificate of Correction** **

TITLE: Wireless telephony for collecting tolls, conducting financial transactions, and authorizing other activities

DATE-ISSUED: November 23, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Morrill, Jr.; Paul H.	Delaware City	DE	19706-0244	

APPL-NO: 08/ 929217   [PALM]
DATE FILED: September 9, 1997

PARENT-CASE:
CROSS-REFERENCE TO RELATED APPLICATION The present application claims the benefit of provisional application Ser. No. 60/020,312 filed in the Patent and Trademark Office on Sep. 11, 1996.

INT-CL: [06] G06 F 15/30, G06 F 15/20, G06 F 15/21, H04 M 11/00

US-CL-ISSUED: 705/44; 705/13, 705/39, 705/40, 705/42
US-CL-CURRENT: 705/44; 705/13, 705/39, 705/40, 705/42

FIELD-OF-SEARCH: 705/13, 705/39, 705/40, 705/42, 705/44

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

▓▓▓ Search Selected ▓▓▓   ▓▓▓ Search ALL ▓▓▓   ▓▓▓ Clear ▓▓▓

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	3652795	March 1972	Wolf et al.	379/91.01
☐	4320387	March 1982	Powell	340/825.34
☐	4341951	July 1982	Benton	705/41
☐	4845636	July 1989	Walker	364/479.07
☐	4926325	May 1990	Benton et al.	705/39
☐	4960981	October 1990	Benton et al.	705/41
☐	5025373	June 1991	Keyser, Jr. et al.	380/24

☐	5157717	October 1992	Hitchcock	379/93.19
☐	5383113	January 1995	Kight et al.	705/40
☐	5465206	November 1995	Hilt et al.	705/40
☐	5485370	January 1996	Moss et al.	395/200.47
☐	5727163	March 1998	Bezos	705/27
☐	5751973	May 1998	Hassett	705/13
☐	5787403	July 1998	Randle	705/43

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
131906	January 1985	EP	

ART-UNIT: 277

PRIMARY-EXAMINER: MacDonald; Allen R.

ASSISTANT-EXAMINER: Myhre; James W.

ATTY-AGENT-FIRM: Connolly Bove Lodge & Hutz

ABSTRACT:

The following procedures describe the use of cellular telephones and other analog
or digital wireless communication devices to conduct transactions and activities.
These procedures effectively allow such devices to function as an electronic
wallet, a wireless PIN pad, and a contactless Smart Card.

8 Claims, 3 Drawing figures

Previous Doc   Next Doc   Go to Doc#

☐ ▓▓▓Generate Collection▓▓▓ | Print |

L12: Entry 1 of 1   File: USPT   Nov 23, 1999

DOCUMENT-IDENTIFIER: US 5991749 A
** See image for **Certificate of Correction** **
TITLE: Wireless telephony for collecting tolls, conducting financial transactions, and authorizing other activities

Abstract Text (1):
The following procedures describe the use of cellular telephones and other analog or digital wireless communication devices to conduct transactions and activities. These procedures effectively allow such devices to function as an electronic wallet, a wireless PIN pad, and a contactless Smart Card.

Application Filing Date (1):
19970909

Brief Summary Text (2):
The present invention relates to methods of using a cellular phone or other wireless communication device to transfer funds between accounts, collect tolls and authorize other activities.

Brief Summary Text (6):
In accordance with the present invention, a method is used to transfer funds between different accounts including the steps of expanding the function of a service provider's central processing unit to include account and authorization information, entering a function code on the keypad of a cellular phone or other wireless communication device, and sending the function code to the central processing unit. The central processing unit identifies the desired transaction and obtains authorization. The central processing unit determines the accounts involved in the transaction, and confirms completion of the transaction.

Brief Summary Text (8):
The desired transaction may involve a default amount at a pre-set price or a variable amount in which case such amount is identified and sent to the central processing unit.

Brief Summary Text (9):
Additionally, in accordance with the present invention, a method is used to verify identity and authorize access to a secured location. This method includes the steps of expanding the function of a service provider's central processing unit to include secure independent verification of a user's identity, and entering a function code on the keypad of a cellular phone or other wireless communication device. The function code is sent to the central processing unit of the provider which identifies the desired transaction as access to a secured location. The desired transaction is authorized and completion of the transaction is confirmed.

Drawing Description Text (3):
FIGS. 1A through 1E comprise flow diagrams illustrating a cell phone transaction/activity procedure, according to the present invention;

<u>Drawing Description Text</u> (5):
FIG. 3A through 3F comprise flow diagrams illustrating a personal computer
<u>transaction</u>/access security procedure, according to the present invention.

<u>Detailed Description Text</u> (2):
The method of the present invention may be used to conduct a number of
<u>transactions,</u> as follows.

<u>Detailed Description Text</u> (3):
Cell Phone Financial <u>Transaction</u> Procedure

<u>Detailed Description Text</u> (4):
Referring in more particularity to FIGS. 1A-1E, the illustrated procedure allows a
cellular phone or other wireless communication device to be used to transfer funds
between accounts belonging to the same entity/person or to an account belonging to
another party. Such <u>transactions</u> could include for example: purchasing a good or
service by transferring funds (paying) to a second party's phone or financial
account; or transferring funds between a person's credit accounts, from credit to
debit or stored-value accounts, to, from, or between bank (saving or checking)
accounts. Other activities could include checking balances in financial accounts.
Communication takes place between the cellular phone and the mobile telephone
service provider's cell antenna and thence via land line to a CPU.

<u>Detailed Description Text</u> (5):
The use of this procedure for these <u>transactions</u> allows the cellular phone to
function as an electronic wallet or as a secure, automated account inquiry
interface. This procedure is carried out by the user first entering a unique
function code on the device's keypad to identify the type of <u>transaction</u> or
activity desired and pressing "SEND." The mobile phone service provider's CPU
identifies the desired <u>transaction</u> and determines if the <u>transaction</u> involves a
default amount (as in a pre-set price for a specific highway toll plaza, transit
fare, or vending machine), which is displayed on the phone's LED screen along with
an "OK?" prompt. User presses "SEND" to continue or "END" to cancel.

<u>Detailed Description Text</u> (6):
If the <u>transaction</u> involves a variable amount (not a specific <u>transaction</u> with a
pre-set default price), such as buying lunch or a souvenir from a street vendor,
the CPU prompts the user to enter an amount, "SEND" it, then prompts "OK?" and the
user presses "SEND" or clears and re-enters amount. The CPU then determines the
types of user accounts to access for the type of <u>transaction</u> and displays either a
default source account <u>authorized</u> to be debited (such as the customers mobile phone
account), or prompts for a unique account code representing a specific credit card,
debit card, bank, or other financial account. The mobile phone service provider CPU
will have a linked record of the customer's pre-<u>authorized</u> financial account
numbers and the customer's written <u>authorization</u> to debit/credit them. The account
code is entered and the user presses "SEND. "

<u>Detailed Description Text</u> (7):
The CPU then determines if the account/<u>transaction</u> protocol requires a personal
identification number (PIN). To prevent unauthorized access and, if so, prompts for
PIN. User enters PIN and presses "SEND." If the <u>transaction</u> type is not linked to a
unique destination account by prior agreement between the mobile service provider
and the 2nd party, the CPU prompts "PAY TO?" and the user enters the account code
to which funds are to be transferred. This destination account code would be a
unique vendor code (made known to the user verbally, by signage or by PC display),
a unique user account code (in the case of an inter-account transfer by a single
party), or the mobile phone number of the recipient.

<u>Detailed Description Text</u> (8):
The user enters the destination account code and presses "SEND." The CPU then

prompts "OK to complete transaction?" and the user presses "SEND" to complete the transaction, or "END" to cancel. The CPU confirms completion of the transaction by generating and displaying a transaction confirmation/authorization number code. If the transaction involves a destination account not linked to the user (a second party's mobile phone account, for example) the CPU will prompt the user to transmit the transaction confirmation/authorization number by pressing "SEND." This number will display on the second party's mobile phone, if the phone is activated, and be transmitted to a pre-authorized computer account. Both parties press "END" to clear the cellular phones for other use.

Detailed Description Text (9):
This procedure permits face-to-face or remote transactions, with immediate confirmation to both parties, for example, the electronic equivalent of paying cash. The CPU debits and credits the appropriate accounts and creates an electronic record of the transfer. The transfer is reflected as a debit on the user's phone bill and as a credit on the recipient's mobile phone statement, along with any phone usage or transaction charges. If the mobile service provider has established a relationship and computer communication link with a bank clearinghouse, credit card issuer, or other financial institution and has the appropriate authorization from the account owner, debits and credits may instead be performed by those institutions and reflected directly on the user's and recipient's bank, credit card, or other periodic bill/statement, with only phone usage or transaction charges, if any, shown on the mobile phone statement.

Detailed Description Text (10):
In performing this procedure, the user may initially enter a unique function code which the CPU identifies as an activity, rather than a transaction, such as checking an account balance. The CPU determines if a PIN is required to prevent unauthorized access to the particular account and, if so, prompts "ENTER PIN. " The user enters PIN and presses "SEND." The remaining steps of this activity would be similar to existing touch tone telephonic automated information procedures, with prompts given visually on the mobile phone LED display, and/or orally by computer.

Detailed Description Text (11):
This procedure may also be used to allow a cellular phone to serve as a security access device. In this case the unique function code would tell the CPU to connect with the predesignated security system computer and prompt the user for the PIN or other access code sequence. The user enters the PIN and presses "SEND." The CPU forwards the authorization to the security computer, which then allows access. The system could allow access based solely upon receiving an authorized PIN or security access code from the user on any cellular phone, or could require that the access code be matched with the specific electronic signature of the cell phone registered to the user. This procedure could apply to a home, building, or area security system with a modem or RF receiver. If equipped with an antenna/receiver (or land line connection) and a processing chip, a garage opener or vehicle security system could also be activated/disarmed by cellular phone, using this procedure.

Detailed Description Text (13):
This example describes the implementation of the cell phone financial transaction procedure for the cash-equivalent purchase of a good or service. For such transactions, the cell phone functions as an electronic wallet, allowing the direct, secure transfer of money between two parties in lieu of cash. Funds are transferred (credited and debited) between the mobile phone accounts of the parties, or may be transferred between other pre-arranged financial accounts such as a credit card account to a bank account or vice-versa. Two cell phones may be used, one for each party to the transaction, or one phone may be used for both parties. The "payor" must initiate the transaction. For the greatest security, the "payor" must use his/her cell phone. This allows the mobile phone service provider to match the required PIN with the specific ID signal of the payor's cell phone. However, the service agreement between the mobile phone service provider and a

customer could provide for account access from other cell phones, if both parties agree.

Detailed Description Text (14):
The payor's funds may be debited to the mobile phone account, from a stored value (pre-paid debit) account with the mobile phone service provider, or from any pre-arranged financial account, such as a bank savings or checking account, a credit card account, or brokerage account. The payor's service agreement with the mobile phone service provider will determine which accounts may be accessed for such transfers. The mobile phone service provider will require the service agreement to include the appropriate financial account number, if any, and written authorization by the customer to debit or credit the appropriate account when a transaction takes place using this procedure. The customer and the mobile phone service provider will jointly establish account codes and PIN that will be used by the customer to conduct an authorized transaction. The periodic billing statements from the mobile phone service provider will include a record of any financial transaction, including date, time, and general location, the nature of the transaction, the amount, the destination account name, the account code of the debited account (if other than the mobile phone account), and any air time or transaction charge which may apply.

Detailed Description Text (16):
The purchaser selects the food desired and is told the amount due by the vendor ("payee"). The purchaser ("payor") activates and/or clears the cell phone for the transaction. The payor presses a function key and the transaction code for a "purchase" ie. a transfer of funds from his account to a second party's account. An example of such a function/transaction code entry might be "* P" (function key plus "P" for "pay bill/transfer funds"). The payor presses SEND. The mobile phone service provider's CPU receives the signal, which includes the ID of the sending phone. Based on this transaction code, the CPU prompts for an amount to be paid or transferred. In this case, the payor has purchased $4.50 worth of food and drink. He enters that amount and presses SEND. The CPU confirms amount and asks "OK?" and the payor presses SEND or clears and corrects the amount and presses SEND. (The payor may press END at any time to cancel the transaction.)

Detailed Description Text (17):
Depending upon the provisions of the service agreement between the customer and the mobile phone service provider, the CPU may then prompt for an account code, representing the account to be debited. This could be automatically set with a default account, such as the payor's mobile phone account, or could be open for any financial account linked via the service agreement with the mobile phone account. In the latter case, the CPU will next prompt for an account code. This code is a shortcut key sequence representing the actual bank or credit card account number, which is on file with the CPU. In this case, the payor has authorized the mobile service provider to debit his checking account and has established the "1" key as the code number representing his checking account. The payor enters "1" and presses SEND. The CPU displays confirmation of the choice of accounts (ie. "CHECKING") and asks "OK?" The payor presses SEND. Depending upon the account code and the service agreement, the CPU may prompt for a PIN. A PIN might not be required for a pre-paid (stored value) account with the mobile phone service provider up to a certain amount such as $20 or $50. But in this case, security requires a PIN. The payor enters his/her PIN and presses SEND. If the PIN corresponds with the cell phone ID, the CPU accepts the identity of the payor and prompts for a destination (to be credited) account code.

Detailed Description Text (19):
In this case, the food vendor has a mobile phone account and has not established a unique vendor code. By signage or verbally, the payee informs the payor of his mobile phone number and the payor enters it at the destination account code prompt and presses SEND. The CPU displays the account code and asks "OK?" and the payor

presses SEND to complete the transaction.

Detailed Description Text (20):
The CPU performs the transaction and displays a confirmation/authorization
number/message. This number/message is a shorthand summary of the transaction
amount and destination account. (An example of this confirmation number/message
might be Jun. 20, 1996 $4.50 8818, this being the transaction date, amount, and
last four digits of the destination phone number.)

Detailed Description Text (21):
The CPU will prompt the payor if he/she wants the confirmation/authorization
number/message sent to the payee. In this case, the payee (the food vendor) has his
mobile phone with him and has it activated. The payor presses SEND and the
Confirmation is displayed on the payee's phone, so he knows the transaction is
correct and has taken place. If the payee does not have a cell phone or does not
have it with him, the payor could simply show the Confirmation message to the payee
on his phone. To end the transaction, the payor presses END.

Detailed Description Text (22):
In this case the payor has elected to debit his checking account. The CPU will
record the transaction and pursuant to the service agreement will direct the bank
to debit/pay the appropriate accounts. The transaction will appear on the payor's
next bank statement. The transaction will also appear on the payor's next cell
phone statement. It might show the date, time, general (cell) location, type of
transaction, destination account code/name, amount, and will include billing for
any air time or transaction fee charged by the mobile phone service provider. If
the payor had elected to debit his mobile phone account, the amount of the
transaction would be added to the total due on his mobile phone bill.

Detailed Description Text (23):
The payee elected to have his mobile phone account credited for the transaction.
His next mobile phone statement would include a record of the transaction and would
show the amount of the transfer as a "credit" to his/her account. The credit could
be used to offset the cost of mobile phone service, or could later be transferred
to a bank account, using this procedure.

Detailed Description Text (25):
This example describes the implementation of the cell phone financial transaction
procedure for the entrance time recording and exit payment by a parking facility
customer. For these transactions under this procedure, the cell phone effectively
functions as a transponder/identifier and as a contactless Smart Card or electronic
wallet. This application of the procedure speeds through-put into and out of the
facility, both for cash and card key customers. It is more convenient for the
customer by not having to take a ticket to enter and handle cash to exit (or
produce a card key). It greatly increases the number of customers a parking company
can serve with automated equipment by expanding the market to include hourly users,
not just monthly account holders. This makes elimination of cashier functions
feasible, reducing personnel, cash handling, and theft costs. This application
could also give the parking company the option of eliminating its monthly billing
system and costs by transferring that function to the mobile phone service
provider.

Detailed Description Text (26):
To allow the fullest use of this procedure, a parking facility with unattended
entrances must have automatic gates which are controllable by computer. The
computers may be at each gate control box or at a central location on or off site.
The computers must be connected to a phone line or must be equipped with an RF
antenna and receiver, so that they can receive information from the mobile phone
service provider's CPU either by land line connection or wireless transmission. The
procedure could, however, also be applied to attended, non-automated facilities as

a means of reducing or eliminating cash <u>transactions</u>.

<u>Detailed Description Text</u> (27):
The parking facility operator will establish an account relationship with the mobile phone service provider. That relationship will define the financial arrangement between the parties relating to customer billing and transfers of payments to an account chosen by the parking provider. The relationship agreement will also establish the unique <u>transaction</u> codes to be used by cell phone users (parking customers) as they enter and exit the parking facility. The financial arrangement will determine, for example, whether customers will be billed by the parking provider, or whether the mobile phone service provider will cause customers to be billed through their cell phone statement or another financial account. Who is liable for, and the level of; any phone usage or <u>transaction</u> fees charged by the mobile phone service provider will also be determined by this financial arrangement.

<u>Detailed Description Text</u> (28):
The unique <u>transaction</u> codes to be used by customers under this procedure would be prominently displayed at the parking facility's entrance and exit gates. For the convenience and safety of customers trying to drive and operate the cell phone, the unique <u>transaction</u> code has as few digits as possible. It is a short-cut key sequence which tells the mobile phone service provider's CPU that this is an entrance/exit parking fee <u>transaction</u> for this particular parking facility and that the fee should be credited to a specific pre-<u>authorized</u> vendor account. Multiple facilities with differing rates would have different unique <u>transaction</u> codes. Different unique <u>transaction</u> codes might also be established for customers paying monthly rates. An example of a shortcut unique <u>transaction</u> code for this application might be *C1'31, meaning a function key (*)+vendor code (here CP for Colonial Parking)+facility ID number (3)+enter/exit code (1 for enter, 2 for exit).

<u>Detailed Description Text</u> (29):
The customer activates or clears the cell phone as he/she approaches the parking facility entrance. A sign announces the availability of pay-by-cell phone and displays the unique <u>transaction</u> code for the facility, which the customer enters on the cell phone and presses "SEND." The unique <u>transaction</u> code (e.g. *CP31) is transmitted to the mobile phone service provider CPU which records the user's identity, the date and time, and the <u>transaction</u> type--here "entrance into Colonial Parking facility number 3." The mobile phone service provider's CPU software records the <u>transaction</u> as "open" until the exit <u>transaction</u> code is received. The CPU generates a <u>transaction</u> confirmation/<u>authorization</u> code number, which is displayed on the user's <u>cell</u> phone. The user presses "END" to clear the phone.

<u>Detailed Description Text</u> (30):
The CPU sends the "entrance"_<u>transaction</u> confirmation/<u>authorization</u> number to the parking facility operator's computer, which records the <u>transaction</u> for capacity control and other management reporting purposes and opens the automatic gate. This communication could be via land line, or by RF transmission if the gate or facility is not connected to the PSTN, but has an antenna and receiver.

<u>Detailed Description Text</u> (31):
When departing the parking facility, the user again activates and clears the cell phone as he/she approaches the exit gate. A sign displays the unique <u>transaction</u> code for the facility exit (e.g.*C1132) . The user enters the code and presses "SEND." The mobile phone service provider's CPU receives the code, records the user's identity, the date and time, the <u>transaction</u> type--here "exit from Colonial Parking facility number 3." The CPU searches for the "open" entrance_<u>transaction</u> and matches it with the exit <u>transaction,</u> calculating the elapsed parking time. Depending upon the arrangement between the parking facility operator and the mobile phone service provider, the CPU may have the parking rates on file and may perform

the billing calculation. If not, the CPU sends the user elapsed parking time to the parking facility computer for calculation and the parking facility computer returns the total of the charges to the mobile phone service provider's CPU.

Detailed Description Text (32):
The CPU displays the amount on the user's cell phone along with an "OK?" prompt. If OK' the user presses "SEND" to complete the transaction. The CPU sends the "exit" transaction confirmation/authorization number to the parking facility computer and displays it on the user's cell phone. The user presses "END" to clear the phone. The parking facility computer receives and records the transaction confirmation/authorization number and opens the exit gate.

Detailed Description Text (33):
The billing process will depend upon the arrangement between the parking facility operator and the mobile phone service provider. The customer may be billed directly by the parking facility operator or the charges debited from his/her pre-paid account with the parking facility operator. Alternatively, the arrangement may call for the mobile phone service provider to direct payment funds to the parking facility operator's account. The source of those payment funds will depend upon the service agreement between the customer and the mobile phone service provider and upon the account authorizations granted by the customer to the provider. The parking charges could be billed on the customer's periodic mobile phone statement or debited from a pre-paid mobile phone account. Or the charges could be debited from a pre-authorized credit card, debit card, or banking account and the transaction reflected on the periodic statements from those accounts. These accounts would be linked in the mobile phone service provider's CPU in accordance with the service agreement and signed customer account access authorizations on file.

Detailed Description Text (34):
The customer's mobile phone statement would reflect the transaction by type and date/time and would include any applicable mobile phone charge or other transaction fee.

Detailed Description Text (35):
In the case of an attended parking facility without computer controlled gates, the procedure can be applied in a variety of ways, depending upon the situation. The approaching driver could enter the unique "entrance" transaction code and when the transaction confirmation/authorization is displayed on the cell phone, show it to the attendant. The transaction confirmation/authorization number can be configured to include a vendor code reference so that the attendant knows the transaction is his. If the attendant is equipped with a cell phone, the mobile phone service provider's CPU could send the same transaction confirmation/authorization number to the attendant. When exiting, the user enters the "exit" transaction code and again shows the attendant the confirmation number, or the attendant has it displayed on his/her cell phone.

Detailed Description Text (36):
In the simplest case, if a "mom and pop" parking facility does not have a vendor relationship with the mobile phone service provider and a unique transaction code, it may still make use of this procedure, if it has a mobile phone account. The driver takes a time-stamped ticket upon entry and when ready to exit, the attendant computes the charges. The user "pays" for parking by entering the unique transaction code for "Pay a bill," enters the amount, and enters the parking facility's's mobile phone number as the destination account. The amount of the transaction would be credited to the parking facility operator's mobile phone statement. The user could show the attendant the transaction confirmation/authorization number on his/her cell phone, or it would be displayed on the attendant's phone, if available.

Detailed Description Text (38):
This example describes the application of the cell phone financial transaction
procedure to the payment of transit fares, focusing on bus transit. For these
transactions, the cell phone effectively functions as a contactless Smart Card.
Unlike a contactless Smart Card, however, the user (rider) does not have to hold a
card in close proximity to a card reader. The cell phone's ability to separate the
fare transaction from the act of boarding the bus reduces the queuing time compared
with the use of contact or contactless Smart Cards, or the payment of cash. This
application of the procedure offers a greater number of payment options to
customers, ranging from debiting a prepaid account with the transit operator or the
mobile phone company, to debiting a credit card or bank account, to adding the fare
charge to the mobile phone bill.

Detailed Description Text (39):
The use of this procedure requires a service arrangement between the transit
operator and the mobile phone service provider. This agreement would set
transaction charges for the use of cell phones to collect fares (and who pays
them). The agreement would establish the destination financial account to which
payments to the transit operator would be credited. It would also determine the
unique transaction code system for users (riders) to enter into their cell phones.
The transit operator's fare structure would be entered into the mobile phone
service provider's CPU and electronically accessible for updating. This fare
structure could be variable by time of day, route, type of rider (for example,
discount pass holder/senior citizen), day of the week, and approximate distance
traveled (zones).

Detailed Description Text (41):
This information is built into the unique transaction code the user enters into
his/her cell phone as the bus approaches (or after getting on the bus, if the
operator has an honor system) . For a transit operator who does not have fares
based on zones or distance traveled, the unique transaction code might be *DT37,
meaning a function key (*)+vendor code (here, DT for Delaware Transit)+route number
(37). Any variable pricing by time, day of the week, or discount pass would be
automatically calculated by the mobile phone service provider's CPU.

Detailed Description Text (42):
In this case, the user would enter the unique transaction code (*DT37) and press
"SEND." The unique transaction code is transmitted to the mobile phone service
provider's CPU, which records the user's identity (and knows if the user is a
discount pass holder), the date and time, approximate location (by receiving cell),
and the transaction type--here--"boarded Route 37 bus." The CPU would calculate the
fare amount and display it with an "OK?" prompt. The user presses "SEND" and the
computer displays a transaction confirmation/authorization number or message on the
cell phone. As the user (rider) boards the bus, he/she shows this message or number
to the driver, much like a "Flash Pass." The user then presses "END" to clear the
cell phone. Users who make a transfer during the trip can press the function key
(*) and the "recall" button to re-display the transaction
confirmation/authorization number/message to show the driver of the next bus.

Detailed Description Text (43):
If the transit operator uses a fare structure which includes zone or distance
charges, then signage at the transit stop must include a location code for the
stop, plus a map or list of destinations on the route and their location codes.
Further, let's assume the transit operator wants to know the specific bus in which
the user is riding and displays a bus ID number on the bus' marquee. In this case,
the unique transaction code might be *DT37526, meaning a function key (*)+vendor
code (DT for Delaware Transit)+route number (37)+origination point (here, zone 5)
+destination point (here, zone 2)+bus ID number (#6 on this route) . The user can
enter all elements of the transaction code, except for the bus ID number, prior to
the arrival of the bus.

Detailed Description Text (44):
The billing process will depend upon the agreement between the transit operator and
the mobile phone service provider. If the transit operator has a pre-paid account
or discount pass program, the user's fare charge could be debited from that account
by the mobile phone service provider's CPU. Otherwise, fare charges could be
credited by the CPU to a pre-authorized financial account. The user's charges could
be added to his/her mobile phone bill and reflected on the periodic statement, plus
any phone usage or transaction fees applicable. Alternatively, the service
agreement between the user and the mobile phone service provider could authorize
these transactions to be debited from a linked financial account, be it a bank
account or a credit card.

Detailed Description Text (45):
In either case, the user's mobile phone statement would reflect the date and time
of the transaction.

Detailed Description Text (47):
This procedure is a more specific application of the procedure used to conduct
financial transactions via cellular phone described above. It allows the collection
of tolls from vehicles using a facility at any speed. The procedure does not
require a toll plaza or other physical structure, collection personnel, or
hardware. However, traffic counting tubes, human spotters, and/or video cameras
would be required for enforcement and revenue/traffic reconciliation.

Detailed Description Text (48):
The cell phone in this case functions as an active transponder communicating with a
cell antenna, or a dedicated roadside receiver, which is connected by land line to
the mobile phone service provider CPU. The cell phone also functions as an
electronic wallet (or contactless Smart Card), transferring funds from the user's
account to the tolling authority and recording the transaction.

Detailed Description Text (49):
Referring to FIGS. 2A and 2B, in this procedure the driver is notified by road
signage that cell phone tolling is ahead and is directed to particular lanes set
aside for such use to maximize through-put. The user turns on, or otherwise clears
the cell phone for tolling. Signage informs the driver of the appropriate unique
function code for the particular facility or toll plaza, which the user enters into
the cell phone. As the driver approaches the toll collection area, he presses
"SEND" to transmit the function code and pay the toll. (If the toll is high, or
there are other transaction security concerns, the procedure may call for the
mobile phone service provider's CPU to prompt the user to enter a PIN and press
"SEND.") The driver may be instructed to press "SEND" at a particular point to
facilitate visual or RF detection enforcement.

Detailed Description Text (50):
The CPU receives the function code, matches it with the mobile phone making the
call (via data sub-channel) and confirms the transaction to the user's cell phone
by LED display of the amount of the toll and/or generating a tone. The user presses
"END" after confirmation to clear the phone for other use. The CPU charges the toll
amount and any phone usage or transaction fees to the user's mobile phone account.
By prior arrangement between the user and the mobile phone service provider,
another linked financial account could be the default account for toll charges. The
recorded transaction would be reflected on the user's mobile phone (or other
financial account) bill. Depending upon the agreement between the user and the
mobile phone service provider, the charges could be treated as a credit transaction
or could be debited against a pre-paid (stored value) deposit and so reflected on
the mobile phone bill.

Detailed Description Text (51):

Personal Computer Transaction Authentication/Security Procedure and PC/Cell Phone
Interface Device Description

Detailed Description Text (52):
This procedure describes the use of a cellular telephone in conjunction with a PC
to provide transaction security for purchases (financial transfers) made via the
Internet or other interactive on-line transaction system. Under this procedure the
cellular phone functions as a "PIN pad," providing authorization and authentication
of funds transfers, without sending credit card account numbers over the Internet
or relying upon potentially "hackable" computer software encryption to prevent
unauthorized access to financial account numbers. This procedure requires that,
unless the PC modem is using a cellular telephone to communicate, an interface
device be connected to the personal computer, or installed internally, which allows
communication between a cellular telephone and the PC via a PCMIA cord connection.
Also required are software add-ons to Net browsers, virtual banking, or other
interactive financial programs to provide user information and prompts consistent
with the cell phone transaction/activity procedures.

Detailed Description Text (54):
Referring to FIGS. 3A-3F the user decides to execute an on-line transaction via
computer, such as purchase from an Internet vendor, pay bills electronically, or
interact with a remote secure-access computer. The personal computer is in
communication with a second party's computer, the desired transaction or activity
has been selected on the PC, and any needed price and destination account/access
code is displayed. For example, the computer displays the vendor's account code
number or telephone account number to which funds will be transferred and prompts
the user to enter the unique function code on his cellular phone, which has been
activated and cleared, but not yet connected to the interface device.

Detailed Description Text (55):
The user activates and clears the cell phone. User enters the function code and
presses "SEND." If the transaction/activity involves a payment and unless there is
a default amount associated with the selected function, the mobile service provider
CPU prompts the user cell phone to enter the amount of the transaction and "SEND."
The CPU confirms amount and asks "OK?" User presses "SEND" to continue or "CLEAR"
to reenter. The mobile service provider CPU determines which linked accounts are
pre- authorized for access under this function and displays either a default source
account code to be debited (such as the customer's mobile phone account), or
prompts for a unique account code representing a specific credit card, debit card,
bank, or other financial account. These accounts are linked by pre-authorization
agreement to the user's mobile phone account. The menu codes for each account are
selected by the user and programmed into the CPU at the time service is established
(or later modified). The user enters the desired account code and presses "SEND."
The CPU determines if a PIN is required for the transaction and prompts for it. The
user enters the PIN and presses "SEND."

Detailed Description Text (56):
The mobile phone service provider CPU next prompts for a destination account code
number. This may be a unique vendor code, assigned by agreement with the mobile
phone service provider, a unique account code (in the case of an inter-account
transfer by a single party), or the mobile phone number of the recipient. This
account code or phone number is displayed on the computer screen by the Internet
vendor or interactive banking program. The user enters the destination account code
on the cell phone and presses "SEND." The mobile phone service provider's CPU then
prompts "OK to complete transaction?" User presses "SEND" on the cell phone to
complete the actual transaction or "END" to cancel. The CPU confirms completion of
the transaction by generating and displaying displays a transaction
confirmation/authorization code number.

Detailed Description Text (57):

The user now connects the cellular phone to the <u>cell</u> phone/PC interface device with a PCMIA cord and presses "SEND" on the cellular phone key pad to transmit the confirmation<u>/authorization</u> code number through the interface device to the computer and via the modem to the receiving party. The user then disconnects the cellular phone from the interface device .and presses "END" to clear the phone. The user closes out the PC software program, terminates the Internet or on-line connection, or prepares for another <u>transaction</u>/activity.

<u>Detailed Description Text</u> (58):
Transmitting the <u>transaction</u> confirmation<u>/authorization</u> code number provides the vendor with independently generated real-time confirmation that an <u>authorized</u> <u>transaction</u> has taken place. Neither the actual originating (debited) account/access number, the actual destination (credited) account/access number, nor the user's PIN are sent over the Internet and possibly intercepted.

<u>Detailed Description Text</u> (59):
An unauthorized user with cloned cellular phone would still need to know the unique function codes, the account codes, and the PIN in order to complete a <u>transaction</u> and have the mobile phone service provider CPU generate a confirmation number. A hacker who might gain access to an unattended PC would find no account numbers or PIN record on the hard drive. The cell phone has in effect served as a stand-alone PIN pad and the actual <u>transaction</u> has taken place offline.

<u>Current US Original Classification</u> (1):
705/44

<u>Current US Cross Reference Classification</u> (2):
705/39

<u>Current US Cross Reference Classification</u> (3):
705/40

CLAIMS:

1. A method of transferring funds between different accounts comprising the steps of expanding the function of a service provider's central processing unit to include account and <u>authorization</u> information, entering a function code on the keypad of a cellular phone or other wireless communication device, sending the function code to the central processing unit of the provider which identifies the desired <u>transaction,</u> determining at the central processing unit whether a personal identification number is needed, and supplying the central processing unit with the personal identification number if needed, <u>authorizing the desired transaction,</u> determining the different accounts involved in the<u> transaction,</u> and confirming completion of the <u>transaction</u>.

2. A method of transferring funds between different accounts as in claim 1 wherein the desired <u>transaction</u> involves a default amount at a pre-set price.

3. A method of transferring funds between different accounts as in claim 1 wherein the desired <u>transaction</u> involves a variable amount, identifying the variable amount, and sending it to the central processing unit.

4. A method of verifying identity and <u>authorizing</u> access to a secured location comprising the steps of expanding the function of a service provider's central processing unit to include secure independent verification of a user's identity, entering a function code on the keypad of a cellular phone or other wireless communication device, sending the function code to the central processing unit of the provider which identifies the desired <u>transaction</u> as access to the secured location, determining at the central processing unit whether a personal identification number is needed, and supplying the central processing unit with the

personal identification number if needed, <u>authorizing the desired transaction,</u> and confirming completion of the <u>transaction</u>.

5. A method of verifying identity and <u>authorizing</u> access to a secured location as. in claim 4 wherein the step of <u>authorizing the desired transaction</u> includes communication with the secured location, and activation of the secured location to grant or deny access thereto.

6. A method of transferring funds between different accounts comprising the steps of expanding the function of a service provider's central processing unit to include account and <u>authorization</u> information, transmitting a function code of a cellular phone or other wireless communication device to the central processing unit of the provider which identifies the desired <u>transaction,</u> determining at the central processing unit whether a personal identification number is needed, and supplying the central processing unit with the personal identification number if needed, <u>authorizing the desired transaction,</u> determining the different accounts involved in the <u>transaction</u>, and confirming completion of the <u>transaction</u>.

7. A method of transferring funds between different accounts as in claim 6 wherein the desired <u>transaction</u> involves a default amount at a pre-set price.

8. A method of transferring funds between different accounts as in claim 6 wherein the desired <u>transaction</u> involves a variable amount, identifying the variable . amount, and sending it to the central processing unit.

Hit List

Your wildcard search against 10000 terms has yielded the results below.
Your result set for the last L# is incomplete.
The probable cause is use of unlimited truncation. Revise your search strategy to use limited truncation.

| Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs |

| Generate OACS |

Search Results - Record(s) 1 through 6 of 6 returned.

☐ 1.   Document ID: US 20010011250 A1

Using default format because multiple data bases are involved.

```
L11: Entry 1 of 6                        File: PGPB              Aug 2, 2001

PGPUB-DOCUMENT-NUMBER: 20010011250
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20010011250 A1


TITLE: DISTRIBUTED NETWORK BASED ELECTRONIC WALLET


PUBLICATION-DATE: August 2, 2001


INVENTOR-INFORMATION:
NAME                           CITY               STATE   COUNTRY   RULE-47
PALTENGHE, CRIS T.             NORTHRIDGE         CA      US
MAMDANI, ALNOOR B.             VENICE             CA      US
TAKATA, MELVIN M.              THOUSAND OAKS      CA      US
HUDDLESTON, GREGORY LEE        HUNTINGTON BEACH   CA      US


US-CL-CURRENT: 705/41
```

| Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De |

☐ 2.   Document ID: US 5991749 A

```
L11: Entry 2 of 6                        File: USPT              Nov 23, 1999

US-PAT-NO: 5991749
DOCUMENT-IDENTIFIER: US 5991749 A
** See image for Certificate of Correction **


TITLE: Wireless telephony for collecting tolls, conducting financial transactions,
and authorizing other activities
```

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De |

3. Document ID: US 5966695 A

L11: Entry 3 of 6   File: USPT   Oct 12, 1999

US-PAT-NO: 5966695
DOCUMENT-IDENTIFIER: US 5966695 A

TITLE: Sales and marketing support system using a graphical query prospect database

Full	Title	Citation	Front	Review	Classification	Date	Reference			Claims	KWIC	Draw De

---

4. Document ID: US 5930764 A

L11: Entry 4 of 6   File: USPT   Jul 27, 1999

US-PAT-NO: 5930764
DOCUMENT-IDENTIFIER: US 5930764 A

TITLE: Sales and marketing support system using a customer information database

Full	Title	Citation	Front	Review	Classification	Date	Reference			Claims	KWIC	Draw De

---

5. Document ID: US 5819092 A

L11: Entry 5 of 6   File: USPT   Oct 6, 1998

US-PAT-NO: 5819092
DOCUMENT-IDENTIFIER: US 5819092 A

TITLE: Online service development tool with fee setting capabilities

Full	Title	Citation	Front	Review	Classification	Date	Reference			Claims	KWIC	Draw De

---

6. Document ID: US 5089959 A

L11: Entry 6 of 6   File: USPT   Feb 18, 1992

US-PAT-NO: 5089959
DOCUMENT-IDENTIFIER: US 5089959 A
** See image for **Certificate of Correction** **

TITLE: Method and system for management of an electronic memory representing
predetermined homogeneous units

Full	Title	Citation	Front	Review	Classification	Date	Reference			Claims	KWIC	Draw De

---

Clear	Generate Collection	Print	Fwd Refs	Bkwd Refs	Generate OACS

Terms	Documents
L10 and (cell$ with number)	6

Display Format: [   ] [Change Format]

Previous Page   Next Page   Go to Doc#

Hit List

⁂⁂

| Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs |

| Generate OACS |

Search Results - Record(s) 1 through 10 of 23 returned.

☐ 1. Document ID: US 6853984 B1

Using default format because multiple data bases are involved.

    L7: Entry 1 of 23   File: USPT   Feb 8, 2005

    US-PAT-NO: 6853984
    DOCUMENT-IDENTIFIER: US 6853984 B1

    TITLE: Method and apparatus for credit card processing via facsimile

    DATE-ISSUED: February 8, 2005

    INVENTOR-INFORMATION:
    NAME   CITY   STATE   ZIP CODE   COUNTRY
    Wilkes; W. Bradley   Alpine   UT

    US-CL-CURRENT: 705/44; 705/26, 705/35, 705/38, 705/39, 705/42

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De |

☐ 2. Document ID: US 6636833 B1

    L7: Entry 2 of 23   File: USPT   Oct 21, 2003

    US-PAT-NO: 6636833
    DOCUMENT-IDENTIFIER: US 6636833 B1
    ** See image for **Certificate of Correction** **

    TITLE: Credit card system and method

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De |

☐ 3. Document ID: US 6343279 B1

    L7: Entry 3 of 23   File: USPT   Jan 29, 2002

    US-PAT-NO: 6343279
    DOCUMENT-IDENTIFIER: US 6343279 B1

    TITLE: System integrating credit card transactions into a financial management
    system

`| Full | Title | Citation | Front | Review | Classification | Date | Reference |` ▓▓▓ ▓▓▓ `| Claims | KWIC | Draw De`

☐ 4. Document ID: US 6324526 B1

L7: Entry 4 of 23   File: USPT   Nov 27, 2001

US-PAT-NO: 6324526
DOCUMENT-IDENTIFIER: US 6324526 B1
** See image for **Certificate of Correction** **

TITLE: System and method for performing secure credit card purchases

`| Full | Title | Citation | Front | Review | Classification | Date | Reference |` ▓▓▓ ▓▓▓ `| Claims | KWIC | Draw De`

☐ 5. Document ID: US 6282522 B1

L7: Entry 5 of 23   File: USPT   Aug 28, 2001

US-PAT-NO: 6282522
DOCUMENT-IDENTIFIER: US 6282522 B1

TITLE: Internet payment system using smart card

`| Full | Title | Citation | Front | Review | Classification | Date | Reference |` ▓▓▓ ▓▓▓ `| Claims | KWIC | Draw De`

☐ 6. Document ID: US 6202055 B1

L7: Entry 6 of 23   File: USPT   Mar 13, 2001

US-PAT-NO: 6202055
DOCUMENT-IDENTIFIER: US 6202055 B1

TITLE: Positive identification display device and scanner for low cost collection
and display of graphic and text data in a secure manner

`| Full | Title | Citation | Front | Review | Classification | Date | Reference |` ▓▓▓ ▓▓▓ `| Claims | KWIC | Draw De`

☐ 7. Document ID: US 6163771 A

L7: Entry 7 of 23   File: USPT   Dec 19, 2000

US-PAT-NO: 6163771
DOCUMENT-IDENTIFIER: US 6163771 A

TITLE: Method and device for generating a single-use financial account number

`| Full | Title | Citation | Front | Review | Classification | Date | Reference |` ▓▓▓ ▓▓▓ `| Claims | KWIC | Draw De`

☐ 8.   Document ID: US 6092057 A

L7: Entry 8 of 23   File: USPT   Jul 18, 2000

US-PAT-NO: 6092057
DOCUMENT-IDENTIFIER: US 6092057 A

TITLE: Unattended POS system for automatic control of bank system rejections

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw D: |

☐ 9.   Document ID: US 6052675 A

L7: Entry 9 of 23   File: USPT   Apr 18, 2000

US-PAT-NO: 6052675
DOCUMENT-IDENTIFIER: US 6052675 A

TITLE: Method and apparatus for preauthorizing credit card type transactions

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw D: |

☐ 10.   Document ID: US 6047270 A

L7: Entry 10 of 23   File: USPT   Apr 4, 2000

US-PAT-NO: 6047270
DOCUMENT-IDENTIFIER: US 6047270 A

TITLE: Apparatus and method for providing account security

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw D: |

| Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS |

Terms	Documents
L4 and (705/44).ccls.	23

Display Format: |-_____| Change Format

Previous Page   Next Page   Go to Doc#

Hit List

Search Results - Record(s) 11 through 20 of 23 returned.

☐ 11.   Document ID: US 6023502 A

Using default format because multiple data bases are involved.

```
L7: Entry 11 of 23                    File: USPT              Feb 8, 2000


US-PAT-NO: 6023502
DOCUMENT-IDENTIFIER: US 6023502 A


TITLE: Method and apparatus for providing telephone billing and authentication over
a computer network


DATE-ISSUED: February 8, 2000


INVENTOR-INFORMATION:
NAME                        CITY              STATE    ZIP CODE     COUNTRY
Bouanaka; Hansali           Tinton Falls      NJ
Rahman; Moshiur             Freehold          NJ


US-CL-CURRENT: 379/114.01; 379/127.01, 379/91.01, 705/26, 705/44
```

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw D

☐ 12.   Document ID: US 6021202 A

```
L7: Entry 12 of 23                    File: USPT              Feb 1, 2000


US-PAT-NO: 6021202
DOCUMENT-IDENTIFIER: US 6021202 A


TITLE: Method and system for processing electronic documents
```

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw D

☐ 13.   Document ID: US 6016476 A

```
L7: Entry 13 of 23                    File: USPT              Jan 18, 2000


US-PAT-NO: 6016476
DOCUMENT-IDENTIFIER: US 6016476 A


TITLE: Portable information and transaction processing system and method utilizing
biometric authorization and digital certificate security
```

`Full | Title | Citation | Front | Review | Classification | Date | Reference ▓▓▓▓▓ ▓▓▓▓▓ Claims | KWIC | Draw De`

□ 14.   Document ID: US 6012048 A

L7: Entry 14 of 23   File: USPT   Jan 4, 2000

US-PAT-NO: 6012048
DOCUMENT-IDENTIFIER: US 6012048 A

TITLE: Automated banking system for dispensing money orders, wire transfer and bill payment

`Full | Title | Citation | Front | Review | Classification | Date | Reference ▓▓▓▓▓ ▓▓▓▓▓ Claims | KWIC | Draw De`

□ 15.   Document ID: US 5991410 A

L7: Entry 15 of 23   File: USPT   Nov 23, 1999

US-PAT-NO: 5991410
DOCUMENT-IDENTIFIER: US 5991410 A

TITLE: Wireless adaptor and wireless financial transaction system

`Full | Title | Citation | Front | Review | Classification | Date | Reference ▓▓▓▓▓ ▓▓▓▓▓ Claims | KWIC | Draw De`

□ 16.   Document ID: US 5991381 A

L7: Entry 16 of 23   File: USPT   Nov 23, 1999

US-PAT-NO: 5991381
DOCUMENT-IDENTIFIER: US 5991381 A

TITLE: Method and apparatus for providing telephone calling card validation over a computer network

`Full | Title | Citation | Front | Review | Classification | Date | Reference ▓▓▓▓▓ ▓▓▓▓▓ Claims | KWIC | Draw De`

□ 17.   Document ID: US 5819226 A

L7: Entry 17 of 23   File: USPT   Oct 6, 1998

US-PAT-NO: 5819226
DOCUMENT-IDENTIFIER: US 5819226 A
** See image for Certificate of Correction **

TITLE: Fraud detection using predictive modeling

`Full | Title | Citation | Front | Review | Classification | Date | Reference ▓▓▓▓▓ ▓▓▓▓▓ Claims | KWIC | Draw De`

☐ 18.   Document ID: US 5748908 A
L7: Entry 18 of 23   File: USPT   May 5, 1998

US-PAT-NO: 5748908
DOCUMENT-IDENTIFIER: US 5748908 A ·

TITLE: Automated, classified expenditure data card recording system

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De |

☐ 19.   Document ID: US 5696909 Á
L7: Entry 19 of 23   File: USPT   Dec 9, 1997

US-PAT-NO: 5696909
DOCUMENT-IDENTIFIER: US 5696909 A

TITLE: Virtual POS terminal

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De |

☐ 20.   Document ID: US 5677955 A
L7: Entry 20 of 23   File: USPT   Oct 14, 1997

US-PAT-NO: 5677955
DOCUMENT-IDENTIFIER: US 5677955 A

TITLE: Electronic funds transfer instruments

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De |

| Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS |

Terms	Documents
L4 and (705/44).ccls.	23

Display Format: |- | Change Format

Previous Page   Next Page   Go to Doc#

Hit List

Search Results - Record(s) 21 through 23 of 23 returned.

☐ 21.   Document ID: US 5615110 A

Using default format because multiple data bases are involved.

```
L7: Entry 21 of 23                    File: USPT              Mar 25, 1997
```

```
US-PAT-NO: 5615110
DOCUMENT-IDENTIFIER: US 5615110 A
```

TITLE: Security system for non-cash transactions

DATE-ISSUED: March 25, 1997

```
INVENTOR-INFORMATION:
NAME              CITY                       STATE    ZIP CODE    COUNTRY
Wong; Kam-Fu      Kwun Tong, Kowloon                              HK
```

US-CL-CURRENT: 705/38; 235/379, 235/380, 340/5.42, 340/7.23, 340/7.55, 379/93.02, 705/44

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

---

☐ 22.   Document ID: US 5311594 A

```
L7: Entry 22 of 23                    File: USPT              May 10, 1994
```

```
US-PAT-NO: 5311594
DOCUMENT-IDENTIFIER: US 5311594 A
```

TITLE: Fraud protection for card transactions

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

---

☐ 23.   Document ID: US 5010485 A

```
L7: Entry 23 of 23                    File: USPT              Apr 23, 1991
```

```
US-PAT-NO: 5010485
DOCUMENT-IDENTIFIER: US 5010485 A
```

TITLE: Apparatus, system and method for creating credit vouchers usable at point of purchase stations

| Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw D |

| Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS |

Terms	Documents
L4 and (705/44).ccls.	23

Display Format: [-] | Change Format |

Previous Page   Next Page   Go to Doc#

L11: Entry 1 of 6   File: PGPB   Aug 2, 2001

DOCUMENT-IDENTIFIER: US 20010011250 A1
TITLE: DISTRIBUTED NETWORK BASED ELECTRONIC WALLET

Abstract Paragraph:
A system, in which information is the primary asset and in which investments may be
made in information, includes multiple data stores for storing different types of a
user's information. The safe, secure and properly <u>authorized</u> transfer of
information while preserving individual privacy is provided. The system also
provides for secure backup and storage, as well as for ubiquitous and nomadic
access to information while maintaining the privacy of such information. A first
data store includes static identification data about a user. A second data store
includes moderately dynamic personal data about the user. A third data store
includes dynamic demographic information data about the user. An electronic wallet
can be used with the system to download selected portions of the data for use by
the user. A method of use of the data includes using the data for billing out
forms, providing services to the user and allowing merchants to selectively target
users for sales while maintaining user anonymity.

Application Filing Date:
19981112

Current US Classification, US Primary Class/Subclass:
705/41

Summary of Invention Paragraph:
[0002] This invention relates to information storage and retrieval systems, and
more particularly, to an electronic system for storage and <u>authorized</u> distribution
of personal information.

Summary of Invention Paragraph:
[0010] In one aspect the invention provides a system for the selective
organization, access to and use of personal data. The system may include a server
having data storage capability for storing different types of personal data in
distinct data stores, i.e., an "information bank", such that the information may be
efficiently used by the consumer and by institutions which the consumer has
<u>authorized</u> to access the data. A first data store may include what is known as
static identification data which is personal to a user such as a consumer and which
is typically necessary for establishing a relationship between the consumer and an
institution. Such a consumer will have a means to access the static identification
data, such as a personal computer, network computer, smart telephone or other
communication device through the Internet or other network connection or wireless
connection. A second data store may include what is known as moderately dynamic
personal data about a user or many users, again a consumer or consumers. This would
typically include a large volume of data which may be difficult to manage and which
is stored primarily for the convenience of the consumer. A third data store may
include dynamic demographic information data about the users or consumers. This
data may be mined from the data stores mentioned above, or may be the result of
information provided by the consumer, for example, in response to surveys.
Typically, this information is valuable to many research and marketing institutions
which may directly or indirectly compensate the consumer for access to the

information.

Summary of Invention Paragraph:
[0014] More specifically, a consumer's financial institution, by the nature of the transactions in which it engages, already has in its possession large amounts of confidential and disclosure-sensitive information. As may be appreciated from the prior description, examples of this type of information include credit card purchases, income data, bank card transactions, loan application/servicing, etc. Thus, it is optimal for the financial institution to maintain principal possession, maintenance and storage of the types of information described previously for consumer authorized use and distribution, while simultaneously achieving, without the introduction of yet another party, the securing of the consumer's personal information in an "information bank."

Summary of Invention Paragraph:
[0015] In accordance with the invention, the consumer's information may be made available through the financial institution's computer network server, thereby allowing convenient "universal" access to the consumer's personal information, i.e., "static identification data". Thus, access to the consumer's information is only limited by access to standardized devices on computer networks, such as personal computers, i.e., PC's, network computers, PDAs, smart telephones and other communications devices which are connected to the financial institution through the Internet or other network connection. More importantly, the present invention eliminates the need for consumers to have direct access to the consumer's own PC, while at the same time providing required security and access authorization controls.

Summary of Invention Paragraph:
[0016] As noted previously, there is also a need to organize and utilize a much broader range of information, including personal information. This type of information further includes data that is commonly associated with an individual, i.e., the "moderately dynamic personal information", and can be accessed by specific types of organizations or entities such as doctors, tax preparers, etc. Essentially, this information is automatically transferred, upon consumer authorization, to another party in a format that can be used.

Summary of Invention Paragraph:
[0018] A portion of the fee charged by the consumer's financial institution for the request and receipt of the consumer information may be used to pay the consumer as an inducement to participate in the transaction. Accordingly, the consumer is investing information for financial and/or non-financial gain. One example of nonfinancial gain might be the receipt of loyalty credits, as in the case of airline mileage points. Therefore, the consumer is remunerated by the financial institution depending on what the business strategy requires.

Summary of Invention Paragraph:
[0019] The system of the information bank can thus provide, in specific aspects, three types of accounts: a courtesy account, a service account, and a value generation account. Basic information can be stored in the information bank courtesy account and used for automated "form filling" services which are useful to the consumer as an easy means for providing personal information to others when and as authorized. This service may also include a digital signing service, a digital signature verification service, and, for example, notary services.

Summary of Invention Paragraph:
[0020] The information bank system's service account is appropriate for larger amounts of consumer generated data which grows steadily over time. The service will provide for secure backup and storage, as well as for "ubiquitous" and "nomadic" access. Service accounts may hold transaction logs, account histories, medical records, insurance information, financial records, etc.

Summary of Invention Paragraph:

[0021] As personal computing devices become more accessible and "connected" through the Internet and other home networks, the requirement for home data storage devices may decrease. Since "standard" consumer software applications such as e-mail and home accounting packages have become readily available across distributed commercial networks, there is now a corresponding need for network based information storage and safekeeping such as is provided in accordance with the invention. One advantage of using networked information storage is that consumers will have access from many locations, and will not have to carry the information with them when they travel, as do people today. The consumer's information can be made securely and privately available, for example, through "set top boxes" i.e., cable system boxes used on television, and having advanced architecture such as RISC based technology, in hotel rooms or on terminals in emergency hospitals upon authorized demand via smart cards or other similar devices.

Summary of Invention Paragraph:

[0023] Another feature of the service account is to provide third party access to otherwise confidential information in the event of accident, emergency, or death. For example, an unconscious accident victim can't provide PIN or biometric access to urgently required medical information. Under these or other appropriate circumstances, the service makes stored medical information such as patient allergies, medications, medical history, etc., available to authorized recipients. This feature also allows estate executors to access information that is required to handle estate matters, for example, private keys.

Summary of Invention Paragraph:

[0024] Storing data in a self describing meta language, such as XML format, facilitates transfer and use of data by third parties. With proper account owner access authorization, the service facilitates access and understanding of stored personal information, which should reduce the dollar and time cost of services provided by third party professional service providers, such as accountants or physicians.

Summary of Invention Paragraph:

[0025] The service account may also include a cryptographic key escrow and recovery service which provides key escrow and recovery service by storing a key pair and certificate copy after these are generated by a browser, or by generating a key pair and certificate and storing a copy. The service then provides a replacement copy of the key pair and certificate in response to an authorized consumer request.

Summary of Invention Paragraph:

[0028] The system of the information bank also provides the ability for consumers to specify certain important events of which they wish to be reminded or notified. The consumer can also define a notification hierarchy or priority, e.g. cell phone, work number, e-mail, home number, etc. and the tenacity built into the system for notification for each event.

Detail Description Paragraph:

[0045] The information banking system which includes a distributed network based electronic wallet provides a means for consumers to interface with both the information bank and third-party providers of goods, services or information who are referred to herein as merchants. In FIG. 1, the consumer 25 is shown either interfacing with an information bank 23 and various merchants or service providers 27. This can be done by the consumer 25 through a home PC or at a walk-up kiosk type device which utilizes smart card technology, Connection to the information bank 23 can be through conventional transmission lines 29 such as telephone lines, cable, wireless communication, etc. Regardless of the type of user interface chosen, the consumer communicates through the network 29, to the information bank

23 and/or the merchants or service provider 27. The network may be a closed
network, accessible only to the consumer 25, the information bank 23 and approved
merchants or providers 27, or it may be a network such as the Internet, where all
transactions are conducted in a secure manner well known in the art through
appropriate encryption. The information bank 23 can be made up of a conventional
server with appropriate data storage. Within the data storage, separate files or
accounts can be defined as will be readily apparent to those of ordinary skill in
the art. Communications between the server and other users/devices is achieved by
conventional means such as a telephone modem, cable modem or other like established
and well known systems.

Detail Description Paragraph:
[0046] In FIG. 1 there is shown an overview of the types of accounts which will be
maintained at the information bank 23 and the types of information retrieval which
the consumer 25 can control. The consumer's authorized information will be either
requested by or relayed to various merchants or service providers 27 consisting of
associations, billers, or financial institutions with whom the consumer 25 wishes
to transact business. One type of consumer account is known as a courtesy account
31 and holds certain home or personal information, such as the name, address, phone
numbers, e-mail address, birthday, social security number, mother's maiden name,
spouse's information and other familial information which is commonly needed to
fill out forms or otherwise identify the consumer to those with whom they do
business. This type of data is typically known however as "static identification
data" as has been described and will become clearer further herein.

Detail Description Paragraph:
[0047] A second type of account is a service account 33 which is maintained for the
benefit of the consumer and contains "moderately dynamic personal data" about the
consumer 25, as well as software programs which can be accessed by the consumer 25,
and which may be accessed or populated by various merchants or service providers 27
as authorized by the consumer 25. For example, banking accounts, insurance
information, tax returns, and other consumer data can be stored in the service
account. This data is characterized by being a large amount of data which is
dynamic and stored over long periods of time. It can be used for functions such as
bill presentment/payment, relationship management, tax preparation, and other
purposes as will become clearer further herein.

Detail Description Paragraph:
[0049] FIG. 2 illustrates, one example, of how the courtesy account can be used as
a form filling service. In this figure, there is a three-way relationship between
the merchant, in this case a doctor 39, the consumer 25 and the information bank
23. First, the merchant, or in this case, a doctor 35 will send a permission
request for information to the consumer 25 through a separate connection 37 which
can be the Internet, a dedicated line, a phone call, etc. The consumer 25 will then
send a permission message, including a verifiable signatures, back to the doctor
39. The doctor 39 will then forward an information request through, for example,
use of communication device, including a now verifiable permission to the
information bank 23. The information bank 23 will verify the permission as being
valid for this particular consumer 25 before forwarding the consumer's personal
information to the doctor's office 39. The information in this scenario is
originally entered by the consumer 25 directly into the information bank 23. It is
also expected that a merchant or a service provider, such as a doctor, who
maintains information about an individual, such as a history of immunizations,
could have such information directly transmitted to the information bank when the
doctor is authorized to do so by his patient. This would give the patient/consumer
the convenience of having the merchant or service provider provide the Information
Bank with a medical history or with update information, such as a recent
immunization, about the patient/consumer without the inconvenience of the
patient/consumer having to manually forward such information to the Information
Bank which would then have to take the additional step of entering the data. This

would also save the doctor the cost of storing the records.

Detail Description Paragraph:
[0050] Of course, this type of service is not limited to form filling. In a more general sense, the Information Bank allows the consumer to grant conditional, single access or limited access to service providers or merchants such as tax specialists, loan brokers, financial planners, and similar entities, which typically use information provided by a consumer. After retrieving the consumer's information, these entities may generate compilations and/or analysis of the consumer's data and, for example, prepare a tax return, loan application or financial plan for the consumer. The service provider could then either return the prepared document to the consumer or directly file documents such as a tax returns if authorized to do so by the consumer. Resulting information might also be incorporated into the consumer's information stored in the Information Bank for future access and/or analysis.

Detail Description Paragraph:
[0051] FIG. 3 depicts the use of the information bank service account 33 to provide a signing service. Such a service may be provided where a consumer 25 requests such a service and provides the service institution with adequate authorization, such as a power to attorney, to provide signatures for the consumer. As shown in this diagram, the consumer 25 forwards an unsigned document to the information bank 33 where cryptographic software 39 which is conventional in nature and well known to those of ordinary skill will be used to authenticate the consumer 25 and generate a signed document for return to the consumer 25. Also, it is expected that the consumer may authorize the information bank to sign certain documents for the consumer which have been transmitted to the bank by third parties. In such a case, the consumer would review the document and instruct the information bank to sign the document. The information bank could then return the document to the consumer or to the third party if requested by the consumer.

Detail Description Paragraph:
[0052] Electronic commerce requires certain trust components be implemented for signing services. More specifically, current digital signing procedures require parties in electronic transactions to provide critical trust components such as encryption and non-repudiation services. The current public key infrastructure (PKI) which is promoted by various vendors involves certificate authorities (CA's). For the power of attorney signature service described above, the information bank would provide the required key and certificate authority without requiring access to any private verification information or key possessed by a consumer, but would instead provide all authentication services through the information bank service. The information bank would in turn require adequate authentication from the individual consumer for execution of the signing service.

Detail Description Paragraph:
[0053] By implementing a digital signing service with appropriate software 39, the information bank 23 can be used to remedy or eliminate many of the issues related to registration, certificate issuance, certificate verification and certificate revocation lists (CRLs). This also reduces the size of the data transfer required for a verified transaction, because a standard certificate includes the certificate holder's identity, the certificate serial number, a certificate holder's expiration dates, a copy of the certificate holder's public key, the identity of the CA, and the CA's digital signature which is used to confirm that the digital certificate was issued by a valid agency.

Detail Description Paragraph:
[0056] As more and more consumers begin to use electronic commerce and related electronic bill paying services, consumers will need to maintain important home records related to these transactions on their own PCs. The consumer may soon have access to and require safe storage for electronic copies of insurance policies and

other legal documents. Many consumers already create large amounts of data with personal financial software, such as those commercially available under the names Quicken or Turbo Tax. The secured backup and storage service provided by the information bank 33 provides the consumer 25 with the capability to safely and securely store important documents on servers which are professionally managed and reside on information bank 23 hardware. Storage remote from the consumers' PC provides a disaster recovery plan and mitigates any problems associated with hard disc crashes, fire or theft.

Detail Description Paragraph:
[0057] FIG. 5 provides an overview diagram of the types of personal financial information which will be resident on or managed by the information bank's secured backup and storage devices. Personal financial information, such as banking, bill presentment, stocks, mutual funds, 401K accounts or IRAs, all collectively identified with the number 43, can be transferred to the information bank through connections 29 under the consumer's control. Legal documents such as insurance policies, wills, deeds, contracts and other electronic commerce documents can also be forwarded to the information bank 23 for secure archival. Electronic artifacts, such as coupons, point of sale receipts, tickets, tokens and other forms of loyalty credits can be made by the consumer 25 and tracked in the information bank 23 in a secured manner. Important medical records will increasingly be created and stored electronically by medical service providers, and such records of consumers' allergies, medications, past x-rays, diagnoses and doctor's notes can be stored by the consumer 25 and securely and confidentially saved at the information bank 23 in the service account 33 for release only as approved by the consumer 25. In the preferred embodiment the consumer 25 would instruct the third party merchant to forward this information directly to the information bank 23 and it would then be stored therein for the consumer. In an alternate embodiment, these financial and personal documents would be moved from the third party merchant to the consumer 25 and then forwarded by the consumer to the information bank 33.

Detail Description Paragraph:
[0059] The information bank 23 can be used to coordinate the consumer 25 information stored in the information bank 23 with third party service providers in order to more conveniently allow the consumer 25 to use the third party services. For example, the information bank 23 may be used to provide software which will facilitate the downloading of certain consumer information to printing services or in case of emergency, to medical providers. The information bank 23 may also be programmed to release this information to, for example, executors of the consumer's estate if previously authorized to do so by the consumer 25. By being able to share information generated by various service providers, the consumer 25 will find that many previously burdensome tasks are now easily accomplished. In the preferred embodiment, this data will be stored in a self-describing format, such as the XML protocol for easy transfer to and use by various third parties.

Detail Description Paragraph:
[0061] The information bank 23 is configured to generally facilitate electronic transactions and make the consumer's life easier and more convenient. The value generation account 35 to be discussed in greater detail hereafter, can be used to provide assisted product, service, or information searches which not only make consumers' lives more convenient, but also provide consumers with some value in return for using the service. This value may be in the form of monetary compensation or it may be in the form of loyalty credits with preferred merchants selected by the consumer 25. This is an optional service and is completely controlled by the consumer 25. The consumer 25 can make their hobbies, personal interest and demographic information available, while keeping their identity private. A consumer profile is compiled by the information bank 23 from both explicit and implicit information. The consumer 25 is given full control and can specify constraints on information and specifically exclude certain information from product, service, or information search categories. Merchant offers which

satisfy the consumer criteria are forwarded by the information bank 23 to the consumer 25. In this system, the merchant will not know the identity or address information of the consumer 25, nor will the consumer 25 know who the identity of the merchant. The information provided must be presented with a summary demonstrating how it satisfies the original interest of the consumer 25 and may include short promotional information. The consumer 25 has the opportunity to request more information or request a purchase. Up to this point, the advertising provided from the merchant to the consumer 25 has been free to the merchant. This allows the merchant to get real time demand statistics and other valuable aggregate indicators of the quality of their offer free of charge. However, in order to complete the final transaction, a fee is required for the merchant to continue. In this way, these advertising dollars are spent by the merchant, knowing they are highly correlated to a targeted sales market.

Detail Description Paragraph:
[0062] FIG. 8 illustrates such a process where the consumer information from the consumer 25 device is entered into the information bank value generation account (previously numeral 35 in FIG. 1) in the form of a profile. In this case, the information bank 23 is shown as consisting of an information bank portion 123 consisting of the courtesy account and service account previously discussed. The information bank 23 will also include the value generation account module, i.e., number 125 herein, an independent consumer advice module 127, a transaction module 129 providing, matching, brokering, consolidation and accounting functions, and a merchant gateway module 131 which connects to the merchant 133. In this embodiment, the value generation account module 125 takes input from the courtesy and service accounts 123 in the form of explicit and implicit (mined) data. The consumer 25 profile is updated from this data and is provided to a module 129 having a matching function running in the information bank 23. The matching function also is connected to receive offers from a merchant gateway module 131 which is connected to the merchant 133. Merchant offers which sufficiently match the consumer 25 profiles will be forwarded by the information bank 23 to the consumer by the module 129 for review. When a consumer 25 indicates interest in a particular offer, they will issue a request or a buy request back to an information bank consolidator function in module 129, which will then forward this to the merchant 133, either individually or in bulk with other consumer offers. The merchant 133 will then pay a fee for the brokerage service and portions of this will be split by the information bank 23 and allocated to particular consumer accounts as appropriate. This function also includes an independent consumer advisor module 127 which includes data available to the consumer 25 for reference, and provides background information about various merchant offers.

Detail Description Paragraph:
[0066] As further shown in FIG. 9, the information bank manufacturer gateway module 144 can be programmed to mint a coupon and issue this via the manufacturer 145 electronically to the consumer 25 who will then store the coupon in the information bank service account 33 or in an electronic wallet therein. Coupons may be issued by manufacturer, distributors and/or retailers, and tickets may be issued, for example by various entertainment and/or educational concerns. Tokens are issued by a wide variety of concerns ranging from transportation authorities to entertainment establishment. Almost any retailer or business could create a loyalty program using tokens. The consumer 25 in receipt of a coupon, ticket or token would store these in a service account or smart card electronic wallet. When the consumer wished to redeem these coupons, they would forward them to the information bank retailer gateway module 137 which presents the coupons to the information bank clearinghouse module 139 for settlement. The information bank manufacturer gateway module 141 then would issue an appropriate credit back through the information bank clearinghouse module 139 to the appropriate retailer 147 in exchange for the redeemed coupon. All of these functions can be implemented routinely by those of ordinary skill in the art using existing hardware and software tools and devices once the broad functionality described in detail herein is known.

Detail Description Paragraph:
[0068] The information bank also provide an anonymous shopping service. This
service, as shown in FIG. 11, allows several components of the information bank
(such as the service account 33, an anonymizer module 153 which assigns an alias to
all consumer transactions, an order payment consolidator module 155, a junk e-mail
investigator module 157 and a reshipper module 159 to work together to provide an
intermediate shopping service which allows the consumer to browse certain merchant
displays over the Internet without revealing their identity. The modules and
functions described are conventional and well known, for example, from such
services already available from certain web service providers. However, to date, no
one has integrated the noted functions and modules into a coherent functioning
system as provided by the present invention.

Detail Description Paragraph:
[0075] At the other end of the spectrum is the totally virtual wallet. It is not a
physical device, but a set of applications on a server somewhere. The major
disadvantage of this approach is that all transactions have to be "on-line" or
connected to a server. This could result in more expensive and/or less convenient
use. Another issue is security.

Detail Description Paragraph:
[0076] A hybrid approach, and that preferred in accordance with the system 21 of
the invention, is to put some data and applications on a physical device and some
on a server. A smart card is ideally suited for this type of application since it
makes the most sense to put the security and access functions on the card, and to
put the volume of data and applications on the server such as the information bank
23. Further, those transactions that would be too expensive to have on-line, such
as small amounts of electronic cash transactions, also makes sense to have on a
such a smart-card. Thus, as shown in FIG. 13, the electronic wallet 171 in one
embodiment is made up of an e-cash applications container 173, an electronic cash
application manager 175, a use or authentication module 177, a key to application
manager 181, a key ring applications container 183, and external applications
interoperability API (applications program interface) 179, and a user application
organizer and manager 185.

Detail Description Paragraph:
[0078] The key to application manager 181 serves to manage non-cash applications in
the wallet such as credit, debit, e-checks, identification, facilities access and
other applications. This is the software that maintains the contents of the key
ring application container 183. The key-ring container 183 holds the connectors to
server applications. The contents are managed and maintained by the key to
application manager 181 previously described. Even as smart cards become more
commonly available, it is believed that they will not be sufficiently large to
actually hold the applications. Instead, they will hold "connectors" to the
applications that reside on a server. The most important aspect of a "connector" is
a key or certificate that helps identify an authorized user of the application. The
"key ring" then is a container of keys. They are not like the "real" keys, however,
as further illustrated by FIG. 14 hereof.

CLAIMS:

5. A system according to claim 1 further comprising authorizing means for allowing
selected users access to and use of dynamic personal information data in said third
data store.

10. A system according to claim 1 wherein said second data store includes credited
value data for use by a user in commercial transaction.

15. A method as in claim 1 further comprising downloading purchasing credits from

said second data store into an electronic wallet to allow a user to engage in commercial transactions with such credits.

18. A method as in claim 1 further comprising authorization by a user to allow selected third parties to access data in said second data store.